Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111
	)	
CellAntenna Corp. Request for Amendment of Section 2.807 of the Commission's Rules (47 C.F.R. § 2.807) to Allow the Use of Radio Frequency Jamming Equipment by Local and State Law Enforcement Agencies and Emergency Response Providers	)	RM-11430
	)	
Petition of The GEO Group, Inc. for Forbearance from Application of Sections 302, 303, and 333 of the Communications Act of 1934, as amended, and Sections 2.803 and 2.807 of the Commission's Rules to Allow State and Local Correctional Authorities to Prevent Use of Commercial Mobile Radio Services at Correctional Facilities	)	ET Docket No. 08-73
	)	
CTIA—The Wireless Association Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammers and Wireless Boosters and Repeaters	)	WT Docket No. 10-4
	)	
South Carolina Department of Corrections Request for Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users	)	PRM09WT
	)	
Mississippi Department of Corrections Request for Authorization of Managed Access Systems Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users	)	PRM09WT
	)	
Global Tel*Link Corp. Request for Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission's Rules and Creation of New Rule(s) to Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities	)	PRM11WT
	)	

Cell Antenna Corp. Request for Amendment of Section 20.5 of the Commission's Rules, 47 C.F.R. § 20.5, to Categorically Exclude Service to Wireless Devices Located on Local, State, or Federal Correctional Facility Premises	)	PRM11WT

COMMENTS OF AT&T, INC.

AT&T Inc. (AT&T), on behalf of its subsidiaries, respectfully submits these comments in response to the Notice of Proposed Rulemaking (NPRM) in the dockets captioned above,[1] wherein the Commission seeks comment on its proposed steps to facilitate the development of solutions to repress the use of contraband wireless devices in correctional facilities nationwide. The Commission has proposed[2]

1. A series of modifications to the Commission's rules to facilitate spectrum lease agreements between wireless providers and providers or operators of managed access systems used to combat contraband wireless devices.
2. A requirement that wireless providers terminate service, if technically feasible, to a contraband wireless device if an authorized correctional facility official notifies the wireless provider of the presence of the contraband wireless device within the correctional facility.

The Commission also solicits comment on other technological approaches for addressing the problem of contraband wireless device usage in correctional facilities.

Overall, AT&T welcomes the proposed steps for streamlining spectrum leasing between wireless carriers and vendors of managed access systems. As described below, AT&T does have some recommendations for further simplification of spectrum leasing in this context and also has proposals for the means by which contraband phones are deactivated.

The Commission makes three proposals for the streamlining of spectrum leases between wireless carriers and managed access vendors.

1. Revision of the Commission's rules to immediately process *de facto* lease agreements or spectrum manager lease agreements for spectrum used exclusively in managed access systems in correctional facilities, and streamlining other aspects of the lease application or notification review process for those managed access systems in correctional facilities.

---

[1]Hereafter collectively referred to as the Managed Access Service NPRM ("MAS"). Several of these dockets seek to permit the use of jamming technologies as a means of blocking contraband wireless devices. *See, e.g.*RM-11430. AT&T urges the Commission to dismiss these proceedings upon the issuance of a final order pursuant to this NPRM.

[2] MAS at ¶¶ 2-3.

2. Forbearance, to the extent necessary, from the individualized application review and public notice requirements of Sections 308, 309, and 310(d) of the Communications Act of 1934, as amended (the Act), for qualifying managed access leases.
3. Establishment of a presumption that managed access operators provide a private mobile radio service (PMRS) and streamlining the process for seeking Special Temporary Authority (STA) to operate a managed access system.[3]

AT&T supports these changes, which it believes will help to reduce the time required and the resources expended by carriers to complete a spectrum lease with managed access and detection system vendors. AT&T, however, would go at least a step further to streamline this process.

AT&T understands the motivation behind the Commission's proposal to require carriers to terminate service to a device suspected of being a contraband device upon request from a corrections official. AT&T certainly will terminate service to a device in compliance with a lawful order from a court or the FCC. Because the FCC cannot lawfully delegate its statutory authority to a third party, such as a state corrections officer, AT&T cannot endorse this proposal.

Background

There are a number of ways to control the problem of contraband wireless device in prisons. Corrections officials presumably already take a number of steps to control the physical security of the facility. Indeed, the steps one would take to prevent inmates from obtaining contraband cellphones would be no different from the steps taken to prevent inmates from obtaining possession of weapons or drugs. In addition to these primary means of preventing inmates from possessing cellphones, officials have explored technical means to prevent inmates from using devices that they manage to obtain notwithstanding prison security measures. Because jamming radio signals is unlawful[4] (and in this context would jam both lawful and unlawful communications), corrections officials and industry have focused on the use of managed access systems and detection systems.

---

[3]MAS at ¶ 2. The Commission also seeks comment on whether to establish a requirement that managed access providers should provide notice to nearby households and businesses prior to activation of a managed access system. *Ibid.* AT&T strongly supports giving such notice to the surrounding community to alert subscribers to the possibility of accidental blocking.

[4] 47 U.S.C. § 333; *see,* MAS n. 74.

Managed access systems are micro-cellular, private networks that analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized for purposes of accessing public carrier networks.[5] When a wireless device attempts to connect to the network from within the coverage area of the managed access system, the system cross-checks the identifying information of the device against a database that lists wireless devices authorized to operate in the coverage area. The system will permit authorized devices to communicate in the usual fashion; unauthorized devices are blocked by the managed access system.

Detection systems generally identify the location of a contraband wireless device through triangulation. As detection systems are passive and can only approximate the location of a contraband device, correctional facility employees must search for and physically confiscate the identified contraband device to terminate operations.[6] Because these searches may impose additional cost and create security issues for prisons, proponents of detection systems seek a rule change to require wireless carriers to terminate service to unauthorized wireless devices discovered by detection systems.[7]

In order to operate managed access systems or detection systems, operators of these private networks require a right to transmit over spectrum exclusively licensed to others for commercial mobile services. Wireless carriers have been willing to lease spectrum rights to these private network operators in an effort to address the problem of contraband devices in prisons, but the leasing rules, while effective for secondary market transactions among commercial providers, are far more cumbersome in the case of managed access providers. In order to effectively control the unlawful use of contraband devices within prisons, managed access or detection system operators must have the right to operate in every spectrum block that might be used by any commercial licensee. This might require leases of 15 to 20 separate licenses to cover a single corrections facility.

---

[5] MAS at 14.
[6] MAS at ¶ 53,
[7] *Id.* at ¶ 54.

1. Spectrum Leasing for Managed Access

AT&T believes that the Commission should recognize that the leases at issue here are of a new kind. Carriers will almost certainly enter into multiple leases of this sort with each managed access vendor. The geographic scope of these leases is extremely limited because the nature of the service is intended to cover only the territory of a correctional institution. Consequently, it is very likely that a wireless carrier entering into such a lease with managed access vendor XYZ for a prison in Texas will replicate that same lease for XYZ's service to prisons in Iowa, California, and other locations. It should be unnecessary to restart the streamlined proceeding for each subsequent lease that the CMRS carrier enters into with vendor XYZ. AT&T therefore proposes that the first lease entered into with a managed access carrier should become the "lead" application. Once approved, the carrier should need only amend the lease to add any new call signs, coordinates for the new license area and such other data the Commission may require.[8] This approach will save all parties – including the Commission – time, effort, and expense while still providing the information needed to track the leases.

In addition to simplifying spectrum leasing, AT&T also recommends that rules make clear that the underlying licensee shall not be required to comply with E-911 requirements within the leased area, under either a spectrum manager or de *facto* transfer lease.[9] Indeed, in this proceeding, the Commission proposes to amend Section 20.9[10] of its rules to establish that managed access services in correctional facilities provided on spectrum leased from wireless providers shall be presumptively treated as PMRS, and not subject to the 911 and E911 rules. In making this proposal, the FCC seeks comment on whether there are potential benefits to applying some or all of the Commission's 911 or E911 rules to a managed access provider operating as a PMRS that transmits 911 or E911 calls on its system.[11] AT&T submits that no

---

[8] The Commission should also waive its leasing rules to the extent necessary to allow licensees with site based authorizations, such as cellular, to enter into geographic area leases; i.e., leases covering license areas defined by lat/long descriptions, rather than site by site. This would allow a single exhibit describing the leased area to be used to cover all licenses to which the lease would apply for a given correctional institution.

[9] 47 C.F.R. § 20.18(a). *See also,* MAS at n. 151.

[10] 47 C.F.R. § 20.9(a)

[11] MAS at § 46.

matter how the Commission decides to resolve this question, the underlying licensee should not be held responsible for 911 or E911 calls originating from anywhere within the area leased to the managed access system operator, whether from contraband devices or not. In the first place, if the FCC exempts the managed access system from the 911 and E911 rules, it makes to no sense to hold the spectrum licensee responsible for those calls. On the other hand, if the managed access system must adhere to some or all of the 911 or E911 rules, it is the managed access system that will have to let the emergency call pass through its system. Again, the spectrum licensee should not bear responsibility for emergency calls that may be captured and blocked by a managed access system, for example.

While AT&T encourages the use of lawful methods to prevent the unlawful use of contraband devices in prisons, the rules that allow the use of spectrum based methods such as managed access and detection systems must ensure that the use of these tools do not cause harmful interference to lawful users of commercial networks. In this regard, the Commission should establish a clear and specific timeline for resolving interference issues. In particular, the operator of a managed access system or a detection system should be required to respond within 24 hours to any notification from a commercial wireless carrier that the operator's system is causing harmful interference to the carrier's network.[12] Moreover, operators of managed access systems or detection systems should be required to shut down their systems immediately upon a request from either the FCC or a commercial wireless operator pending the resolution of such interference.[13]

2. Deactivation of Contraband Devices

AT&T's wireless service agreements give the company the right to terminate service to any subscriber who uses it in an unlawful manner. AT&T will do so in appropriate circumstances. To date, AT&T has received few requests to deactivate wireless devices believed to be contraband devices operating un-

[12] *See, e.g.,* 47 C.F.R. § 90.674(a)(3) and the procedures described there.

[13] Such requirements are not unusual in the case of operators of devices using commercial mobile frequencies that have the potential to cause harmful interference to commercial mobile networks. *See, e.g.,* 47 C.F.R. § 90.219(b)(1)(ii)("However, signal booster operation is on a non-interference basis and operations may be required to cease or alter the operating parameters due to a request from an FCC representative or a licensee's request to resolve interference."). Of course, licensees should remain free to include interference abatement procedures in any spectrum lease document.

lawfully. However, as managed access and detection systems become more widespread, AT&T expects the number of these requests to mount. This is especially true with detection systems that can identify wireless devices being used within the signal range of their systems, but which, unlike managed access systems, have no capability to capture and block calls suspected of originating from within a correctional institution. In such cases, the operator of a detection system may be likely to request that the wireless carrier to which the suspect device is subscribed deactivate the device.[14]

Carriers faced with such requests for termination are confronted with a dilemma. In the absence of a court order or an order from the FCC compelling them to terminate service,[15] the carrier must, of course, investigate the request to determine whether the device appears to be contraband—a device possessed unlawfully by an inmate or used unlawfully within a correctional institution. To the extent that the device appears to have been used recently on its network, it may be likely that the device was identified because it traveled into range of a detection system (or was captured by a managed access system), even though it might never have been used, lawfully or otherwise, within a correctional institution. In such a case, the deactivation of a legitimate account by a carrier could result in endangering the safety of a law-abiding user, not to mention engendering disputes, potential liability and reputational harm. In short, in the absence of a lawful order requiring service termination, it is the carrier that must risk the consequences of terminating service to a device, so it is the carrier that must ultimately determine whether there is sufficient proof of unlawful use to justify deactivating the device. To point this out is not to minimize the serious problems presented to correctional facilities and personnel by the operation of contraband wireless devices. Rather, it is to underscore that a carrier is likely in a better position to determine whether a device identified as "contraband" has been mistakenly caught or identified by the managed access system. In addition, it is the carrier that must risk the consequences of terminating service in such cases. Accordingly, in an absence of a lawful order compelling termination, it is the carrier who must decide.

---

[14] Indeed, as noted above, proponents of detection systems seek a rule change to *require* carriers to terminate service to wireless devices upon the demand of a prison official.

[15] *See, e.g.* 47 U.S.C. § 4(i).

In the NPRM, the Commission proposes to resolve this dilemma by simply *requiring* commercial wireless carriers to terminate service to any device provided it has received a "qualifying request" from an "authorized party."[16] The "authorized party" would be a prison official.[17]

The Commission argues in the NPRM that it has the authority under Section 303[18] to require carriers to terminate service to contraband wireless devices.[19] AT&T does not dispute this analysis and, were the order to terminate service issued by the FCC, AT&T would, of course, comply with it. The FCC may not, however, delegate this authority to a third party, such as a corrections officer or managed access system operator. The Communications Act permits the FCC to delegate its functions to "a panel of commissioners, an individual commissioner, an employee board, or an individual employee."[20] The "authorized person" described in the NPRM is none of those things, but would be an unrelated third party. The FCC lacks the authority to delegate its powers to a third party.

To support its approach, the Commission notes a "nexus between this proposal and the wireless industry's recent voluntary commitment to take steps to help deter smartphone thefts and protect consumer data."[21] However, in the case of a stolen phone or customer data, it is the subscriber who requests the carrier to take some action and not an unrelated third party purportedly "authorized" by the FCC. When a subscriber directs her carrier to undertake some action on her own account, a carrier may be confident that she will ratify the action taken. By contrast, the NPRM proposes that a carrier be required to terminate service not at the direction of its customer, a court or the Commission itself, but at the request of a prison official. While a carrier may honor such a request, it cannot be required to do so.

This is not to say that AT&T will not continue to work with corrections officials to help prevent the use of contraband phones in prisons. AT&T will continue to review any requests it might receive from prison officials seeking to deactivate devices believed to be contraband. It is merely to say that in the

---

[16]MAS at ¶ 56.
[17]*Ibid.*
[18] 47 U.S.C. § 303
[19]MAS at § 60.
[20]47 U.S.C. § 155(c)(1)
[21]*Id.* at 57.

absence of a lawful order compelling it to terminate service to a device, the carrier itself must decide whether to terminate service.

Conclusion

For the foregoing reasons, AT&T respectfully urges the Commission to adopt the streamlined licensing procedures it has proposed in this NPRM as well as AT&T's additional suggestions. In addition, the interference protections proposed by AT&T should also be adopted. Finally, AT&T urges the Commission not to require carriers to act on the termination orders issued by prison officials. The Commission cannot delegate this authority and carriers need to verify, to the extent possible, the accuracy of such a request.

Respectfully submitted,

William L. Roughton, Jr.
Michael P. Goggin
Gary L. Phillips
Margaret E. Garber
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036
(202) 457-2040 (phone)
Counsel for AT&T Inc.

July 17, 2013